



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|--------------------------|------------------|
| 10/605,173 | 09/12/2003 | ASHOT ANDREASYAN | PR 1803.01 US | 2172 |
| 31883 | 7590 | 01/17/2007 | | |
| DVA/PIONEER RESEARCH CENTER USA, INC. 2265 E. 220TH STREET LONG BEACH, CA 90810 | | | EXAMINER HA, LEYNNA A | |
| | | | ART UNIT 2135 | PAPER NUMBER |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|--|------------|---------------|
| 3 MONTHS | 01/17/2007 | PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

| | | | | |
|------------------------------|------------------------|--|---------------------|--|
| Office Action Summary | Application No. | | Applicant(s) | |
| | 10/605,173 | | ANDREASYAN, ASHOT | |
| | Examiner | | Art Unit | |
| | LEYNNA T. HA | | 2135 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on _____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 September 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>9/22/2003</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-32 have been examined and is pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. **Claims 1-8 17-32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.**

Claim 1 discloses a method for generating a shared key that includes performing a first and second exponentiation operation to generate a key. The claimed method is directed to an abstract idea because the claim does not require any physical transformation and the invention does not produce a useful, concrete, and tangible result.

MPEP recites:

Practical Application That Produces a Useful, Concrete, and Tangible Result

For purposes of an eligibility analysis, a physical transformation “is not an invariable requirement, but merely one example of how a mathematical algorithm [or law of nature] may bring about a useful application.” AT &T, 172 F.3d at 1358-59, 50 USPQ2d at 1452. If USPTO personnel determine that the claim does not entail the transformation of an article, then USPTO personnel shall review the claim to determine it produces a useful, tangible, and concrete result. In making this determination, the focus is not on whether the steps taken to achieve a particular result are useful,

Art Unit: 2135

tangible, and concrete, but rather on whether the final result achieved by the claimed invention is “useful, tangible, and concrete.” In other words, the claim must be examined to see if it includes anything more than a 35 U.S.C. 101 judicial exception. If the claim is directed to a practical application of a 35 U.S.C. 101 judicial exception, USPTO personnel must then determine whether the claim preempts the judicial exception. If USPTO personnel do not find such a practical application, then USPTO personnel have determined that the claim is nonstatutory. In determining whether a claim provides a practical application of a 35 U.S.C. 101 judicial exception that produces a useful, tangible, and concrete result, USPTO personnel should consider and weigh the following factors:

a) "USEFUL RESULT"

For an invention to be “useful” it must satisfy the utility requirement of section 101.

The USPTO’s official interpretation of the utility requirement provides that the utility of an invention has to be (i) specific, (ii) substantial and (iii) credible. MPEP § 2107 and Fisher, 421 F.3d at 1372, 76 USPQ2d at 1230 (citing the Utility Guidelines with approval for interpretation of “specific” and “substantial”). In addition, when the examiner has reason to believe that the claim is not for a practical application that produces a useful result, the claim should be rejected, thus requiring the applicant to distinguish the claim from the three 35 U.S.C. 101 judicial exceptions to patentable subject matter by specifically reciting in the claim the practical application. In such cases, statements in the specification describing a practical application may not be sufficient to satisfy the requirements for section 101 with respect to the claimed invention. Likewise, a claim that can be read so broadly as to include statutory and nonstatutory subject matter must be amended to limit the claim to a practical application. In other words, if the specification discloses a practical application of a section 101 judicial exception, but the claim is broader than the disclosure such that it does not require a practical application, then the claim must be rejected.

Art Unit: 2135

b) "TANGIBLE RESULT"

The tangible requirement does not necessarily mean that a claim must either be tied to a particular machine or apparatus or must operate to change articles or materials to a different state or thing. However, the tangible requirement does require that the claim must recite more than a 35 U.S.C. 101 judicial exception, in that the process claim must set forth a practical application of that judicial exception to produce a real-world result. *Benson*, 409 U.S. at 71-72, 175 USPQ at 676-77 (invention ineligible because had "no substantial practical application."). "[A]n application of a law of nature or mathematical formula to a ... process may well be deserving of patent protection." *Diehr*, 450 U.S. at 187, 209 USPQ at 8 (emphasis added); see also *Corning*, 56 U.S. (15 How.) at 268, 14 L.Ed. 683 ("It is for the discovery or invention of some practical method or means of producing a beneficial result or effect, that a patent is granted . . ."). In other words, the opposite meaning of "tangible" is "abstract."

c) "CONCRETE RESULT"

Another consideration is whether the invention produces a "concrete" result. Usually, this question arises when a result cannot be assured. In other words, the process must have a result that can be substantially repeatable or the process must substantially produce the same result again. *In re Swartz*, 232 F.3d 862, 864, 56 USPQ2d 1703, 1704 (Fed.Cir. 2000) (where asserted result produced by the claimed invention is "irreproducible" claim should be rejected under section 101). The opposite of "concrete" is unrepeatable or unpredictable. Resolving this question is dependent on the level of skill in the art. For example, if the claimed invention is for a process which requires a particular skill, to determine whether that process is substantially repeatable will necessarily require a determination of the level of skill of the ordinary artisan in that field. An appropriate rejection under 35 U.S.C. 101 should be accompanied by a lack of enablement rejection under 35 U.S.C. 112, paragraph 1, where the invention cannot operate as intended without undue experimentation. See *infra*.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Immonen (US 6,931,528).

As per claim 1:

Immonen discloses the method for generating a shared key comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters; **(see Figure 1 and 2 showing the 1st and 2nd certificates and its parameters)**

performing a first exponentiation operation to generate a first public key from the second peer using at least one parameter of the plurality of first parameters and a first private key from the second peer; **(col.3, lines 10-17 and 59-61; discusses the 1st certificate as CA)**

providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters; **(col.3, lines 19-24; discusses the 2nd certificate as CB)**

Art Unit: 2135

performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters; **(col.3, lines 17-18 and 24-25)**

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. **(col.3, lines 59-66 and col.4, lines 2-8)**

Immonen discloses B generates a random number which is a pre-master key, encrypts it with A's public key, and send the result to A. Now A decrypts this pre-master secret where this server key exchange procedure resembles a mirror image of the one used in TLS, whereby the handshake can still be accomplished with two messages (col.3, lines 59-66). Hence, it would have been obvious for a person of ordinary skills in the art that Immonen reads on the claimed the shared secret key for the first peer using the public key in the third exponentiation operation because as the third exponentiation operation, the decryption key resembles a mirror image of the key used in the TLS.

As per claim 2: See col.3, lines 44-45; discussing the method according to claim 1 wherein the first certificate is a DSA type certificate.

As per claim 3: See col.3, lines 59-61 and col.4, lines 32-40; discussing the method according to claim 2 wherein the first and second parameters comprise a prime number $p_{sub.dss}$, a prime number $q_{sub.dss}$ a generator $g_{sub.dss}$ and a public key for the first and second

Art Unit: 2135

peers, respectively.

As per claim 4: See col.3, lines 23-26; discussing the method according to claim 3 wherein the first exponentiation operation to generate the first public key is $Y_{sub.R} = g_{sub.dss} \{ \text{circumflex over ()} X_{sub.R} \text{ mod } p_{sub.dss} \}$ where $X_{sub.R}$ is a one-time private key from the second peer.

As per claim 5: See col.2, lines 3-6 and col.3, lines 17-19; discussing the method according to claim 4 wherein the second exponentiation operation to generate the shared secret key for the second peer is $_{sub.SSK} = Y_{sub.Adss} \{ \text{circumflex over ()} X_{sub.R} \text{ mod } p_{sub.dss} \}$ where $Y_{sub.Adss}$ is a DSS public key from certificate of peer A.

As per claim 6: See col.3, lines 17-19; discussing the method according to claim 5 wherein $Y_{sub.Adss} = g_{sub.dss} \{ \text{circumflex over ()} X_{sub.Adss} \text{ mod } p_{sub.dss} \}$ where $X_{sub.Adss}$ is a DSS private key from certificate of peer A.

As per claim 7: See col.3, lines 24-25 and col.4, lines 2-8; discussing the method according to claim 5 wherein the third exponentiation operation to generate the shared secret key for the first peer is $Y_{sub.SSK} = Y_{sub.R} \{ \text{circumflex over ()} X_{sub.Adss} \text{ mod } p_{sub.dss} \}$ where $X_{sub.Adss}$ is a DSS private key from certificate of peer A.

As per claim 8: See col.4, lines 44-45; discussing the method according to claim 1 wherein the first and second certificates are sent to

Art Unit: 2135

the second and first peers, respectively, over a wireless network.

As per claim 9:

Immonen discloses the article of manufacture comprising:

a machine accessible medium including data that, when accessed by a machine, causes the machine to perform operations comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters; **(see Figure 1 and 2 showing the 1st and 2nd certificates and its parameters)**

performing a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer; **(col.3, lines 10-17 and 59-61; discusses the 1st certificate as CA)**

providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters; **(col.3, lines 19-24; discusses the 2nd certificate as CB)**

performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters; **(col.3, lines 17-18 and 24-25)**

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. **(col.3, lines 59-66 and col.4, lines 2-8)**

Art Unit: 2135

Immonen discloses B generates a random number which is a pre-master key, encrypts it with A's public key, and send the result to A. Now A decrypts this pre-master secret where this server key exchange procedure resembles a mirror image of the one used in TLS, whereby the handshake can still be accomplished with two messages (col.3, lines 59-66). Hence, it would have been obvious for a person of ordinary skills in the art that Immonen reads on the claimed the shared secret key for the first peer using the public key in the third exponentiation operation because as the third exponentiation operation, the decryption key resembles a mirror image of the key used in the TLS.

As per claim 10: See col.3, lines 44-45; discussing the article of manufacture according to claim 9 wherein the first certificate is a DSA type certificate.

As per claim 11: See col.3, lines 59-61 and col.4, lines 32-40; discussing the article of manufacture according to claim 10 wherein the first and second parameters comprise a prime number $p_{sub.dss}$, a prime number $q_{sub.dss}$, a generator $g_{sub.dss}$ and a public key for the first and second peers, respectively.

As per claim 12: See col.3, lines 23-26; discussing the article of manufacture according to claim 11 wherein the first exponentiation operation to generate the first public key is $Y_{sub.R} = g_{sub.dss}^{\text{circumflex over ()} X_{sub.R}} \text{ mod } p_{sub.dss}$ where $X_{sub.R}$ is a one-time private key from the second peer.

Art Unit: 2135

As per claim 13: See col.2, lines 3-6 and col.3, lines 17-19;

discussing the article of manufacture according to claim 12 wherein the second exponentiation operation to generate the shared secret key for the second peer is $Y_{\text{sub}}.\text{SSK} = Y_{\text{sub}}.\text{Adss}\{\text{circumflex over ()}\}X_{\text{sub}}.\text{R} \bmod p_{\text{sub}}.\text{dss}$ where $Y_{\text{sub}}.\text{Adss}$ is a DSS public key from certificate of peer A.

As per claim 14: See col.3, lines 17-19; discussing the article of manufacture according to claim 13 wherein

$Y_{\text{sub}}.\text{Adss} = g_{\text{sub}}.\text{dss}\{\text{circumflex over ()}\}X_{\text{sub}}.\text{Adss} \bmod p_{\text{sub}}.\text{dss}$ where $X_{\text{sub}}.\text{Adss}$ is a DSS private key from certificate of peer A.

As per claim 15: See col.3, lines 24-25 and col.4, lines 2-8;

discussing the article of manufacture according to claim 13 wherein the third exponentiation operation to generate the shared secret key for the first peer is $Y_{\text{sub}}.\text{SSK} = Y_{\text{sub}}.\text{R}\{\text{circumflex over ()}\}X_{\text{sub}}.\text{Adss} \bmod p_{\text{sub}}.\text{dss}$ where $X_{\text{sub}}.\text{Adss}$ is a DSS private key from certificate of peer A.

As per claim 16: See col.4, lines 44-45; discussing the article of manufacture according to claim 9 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

As per claim 17:

Art Unit: 2135

Immonen discloses a system comprising:

a processor; and a memory coupled to the processor, the memory containing program code that, when executed by the processor, causes the processor to: **(col.4, lines 59-65 and Figure 2; shows the memory coupled to the processor B')**

provide a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters; **(see Figure 1 and 2 showing the 1st and 2nd certificates and its parameters)**

perform a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer; **(col.3, lines 10-17 and 59-61; discusses the 1st certificate as CA)**

provide a second certificate and the first public key from the second peer to the first peer; **(col.3, lines 19-24; discusses the 2nd certificate as CB)**

the second certificate comprising a plurality of second parameters;

perform a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters; **(col.3, lines 17-25)**

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. **(col.3, lines 59-66 and col.4, lines 2-8)**

Art Unit: 2135

Immonen discloses B generates a random number which is a pre-master key, encrypts it with A's public key, and send the result to A. Now A decrypts this pre-master secret where this server key exchange procedure resembles a mirror image of the one used in TLS, whereby the handshake can still be accomplished with two messages (col.3, lines 59-66). Hence, it would have been obvious for a person of ordinary skills in the art that Immonen reads on the claimed the shared secret key for the first peer using the public key in the third exponentiation operation because as the third exponentiation operation, the decryption key resembles a mirror image of the key used in the TLS.

As per claim 18: See col.3, lines 44-45; discussing the system according to claim '17 wherein the first certificate is a DSA type certificate.

As per claim 19: See col.3, lines 59-61 and col.4, lines 32-40; discussing the system according to claim 18 wherein the first and second parameters comprise a prime number $p_{\text{sub.dss}}$, a prime number $q_{\text{sub.dss}}$, a generator $g_{\text{sub.dss}}$ and a public key for the first and second peers, respectively.

As per claim 20: See col.3, lines 23-26; discussing the system according to claim 19 wherein the first exponentiation operation to generate the first public key is $Y_{\text{sub.R}} = g_{\text{sub.dss}}^{\text{circumflex} x \text{ over } (}}$ $X_{\text{sub.R}} \bmod p_{\text{sub.dss}}$ where $X_{\text{sub.R}}$ is a one-time private key from the second peer.

Art Unit: 2135

As per claim 21: See col.2, lines 3-6 and col.3, lines 17-19;

discussing the system according to claim 20 wherein the second exponentiation operation to generate the shared secret key for the second peer is $Y_{\text{sub}}.\text{SSK} = Y_{\text{sub}}.\text{dss}\{\text{circumflex over ()}\}X_{\text{sub}}.R \bmod p_{\text{sub}}.\text{dss}$ where $Y_{\text{sub}}.\text{Adss}$ is a DSS public key from certificate of peer A.

As per claim 22: See col.3, lines 17-19; discussing the system according to claim 21 wherein $Y_{\text{sub}}.\text{Adss} = g_{\text{sub}}.\text{dss}\{\text{circumflex over ()}\}X_{\text{sub}}.\text{Adss}$ where $X_{\text{sub}}.\text{Adss}$ is a DSS private key from certificate of peer A.

As per claim 23: See col.3, lines 24-25 and col.4, lines 2-8;

discussing the system according to claim 21 wherein the third exponentiation operation to generate the shared secret key for the first peer is $Y_{\text{sub}}.\text{SSK} = Y_{\text{sub}}.R\{\text{circumflex over ()}\}X_{\text{sub}}.\text{Adss} \bmod p_{\text{sub}}.\text{dss}$ where $X_{\text{sub}}.\text{Adss}$ is a DSS private key from certificate of peer A.

As per claim 24: See col.4, lines 44-45; discussing the system according to claim 17 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

As per claim 25:

Immonen discloses a method comprising:

receiving a first certificate including a plurality first parameters;

(see Figure 1 showing the 1st and 2nd certificates and parameters)

performing a first exponentiation operation to generate a first public key using at least one parameter of the plurality of first

Art Unit: 2135

parameters and a first private key; **(col.3, lines 10-17 and 59-61;**

discusses the 1st certificate as CA)

receiving a second certificate and the first public key, the second certificate including a plurality of second parameters; **(col.3, lines 19-**

24; discusses the 2nd certificate as CB)

performing a second exponentiation operation to generate a first shared secret key using at least one parameter from the plurality of first parameters; **(col.3, lines 17-25)**

performing a third exponentiation operation to generate a second shared secret key using the first public key and a private key. **(col.3, lines 59-66 and col.4, lines 2-8)**

Immonen discloses B generates a random number which is a pre-master key, encrypts it with A's public key, and send the result to A. Now A decrypts this pre-master secret where this server key exchange procedure resembles a mirror image of the one used in TLS, whereby the handshake can still be accomplished with two messages (col.3, lines 59-66). Hence, it would have been obvious for a person of ordinary skills in the art that Immonen reads on the claimed the shared secret key for the first peer using the public key in the third exponentiation operation because as the third exponentiation operation, the decryption key resembles a mirror image of the key used in the TLS.

As per claim 26: See col.3, lines 44-45; discussing the method according to claim 25 wherein the first certificate is a DSA type

Art Unit: 2135

certificate.

As per claim 27: See col.3, lines 59-61 and col.4, lines 32-40;

discussing the method according to claim 26 wherein the first and second parameters each comprises a prime number $p_{sub}dss$, a prime number $q_{sub}dss$, a generator $g_{sub}dss$ and a public key.

As per claim 28: See col.3, lines 17-19; discussing the method according to claim 27 wherein the first exponentiation operation to generate the first public key is $Y_{sub}R = g_{sub}dss^{\circlearrowleft X_{sub}R} \text{ mod } P_{sub}dss$ where $X_{sub}R$ is a one-time private key.

As per claim 29: See col.2, lines 3-6 and col.3, lines 17-19;

discussing the method according to claim 28 wherein the second exponentiation operation to generate the first shared secret key for the second peer is $._{sub}SSK = Y_{sub}Adss^{\circlearrowleft X_{sub}R} \text{ mod } p_{sub}dss$ where $Y_{sub}Adss$ is a DSS public key.

As per claim 30: See col.1, lines 57-58 and col.3, lines 17-19;

discussing the method according to claim 29 wherein

$Y_{sub}Adss = g_{sub}dss^{\circlearrowleft X_{sub}Adss} \text{ mod } p_{sub}dss$ where $X_{sub}Adss$ is a DSS private key.

As per claim 31: See col.3, lines 24-25 and col.4, lines 2-8;

discussing the method according to claim 29 wherein the third

exponentiation operation to generate a second shared secret key is

$Y_{sub}SSK = Y_{sub}R^{\circlearrowleft X_{sub}Adss} \text{ mod } p_{sub}dss$ where $X_{sub}Adss$ is a DSS private key.

Art Unit: 2135

As per claim 32: See col.4, lines 44-45; discussing the method according to claim 25 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100